United States Government Accountability Office

GAO

Testimony
Before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 2 p.m. EDT
Wednesday, October 17, 2007

CRITICAL INFRASTRUCTURE PROTECTION

Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain

Statement of Gregory C. Wilshusen
Director, Information Security Issues

GAO
Accountability * Integrity * Reliability

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-08-119T, a testimony before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Control systems—computer-based systems that monitor and control sensitive processes—perform vital functions in many of our nation's critical infrastructures such as electric power generation, transmission, and distribution; oil and gas refining; and water treatment and distribution. The disruption of control systems could have a significant impact on public health and safety, which makes securing them a national priority.

GAO was asked to testify on portions of its report on control systems security being released today. This testimony summarizes the cyber threats, vulnerabilities, and the potential impact of attacks on control systems; identifies private sector initiatives; and assesses the adequacy of public sector initiatives to strengthen the cyber security of control systems. To address these objectives, GAO met with federal and private sector officials to identify risks, initiatives, and challenges. GAO also compared agency plans to best practices for securing critical infrastructures.

What GAO Recommends

In its report, GAO recommends that DHS improve coordination of control systems activities and information sharing (see table). DHS neither agreed nor disagreed with these recommendations, but stated that it would take them under advisement. The agency also discussed new initiatives to develop plans and processes that are consistent with GAO recommendations.

To view the full product, including the scope and methodology, click on GAO-08-119T. For more information, contact Gregory C. Wilshusen at wilshuseng@gao.gov or at (202) 512-6244.

October 17, 2007

CRITICAL INFRASTRUCTURE PROTECTION

Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain

What GAO Found

Critical infrastructure control systems face increasing risks due to cyber threats, system vulnerabilities, and the serious potential impact of attacks as demonstrated by reported incidents. Threats can be intentional or unintentional, targeted or nontargeted, and can come from a variety of sources. Control systems are more vulnerable to cyber attacks than in the past for several reasons, including their increased connectivity to other systems and the Internet. Further, as demonstrated by past attacks and incidents involving control systems, the impact on a critical infrastructure could be substantial. For example, in 2006, a foreign hacker was reported to have planted malicious software capable of affecting a water filtering plant's water treatment operations. Also in 2006, excessive traffic on a nuclear power plant's control system network caused two circulation pumps to fail, forcing the unit to be shut down manually.

Multiple private sector entities such as trade associations and standards setting organizations are working to help secure control systems. Their efforts include developing standards and providing guidance to members. For example, the electricity industry has recently developed standards for cyber security of control systems and a gas trade association is developing guidance for members to use encryption to secure control systems.

Federal agencies also have multiple initiatives under way to help secure critical infrastructure control systems, but more remains to be done to coordinate these efforts and to address specific shortfalls. Over the past few years, federal agencies have initiated efforts to improve the security of critical infrastructure control systems. However, there is as yet no overall strategy to coordinate the various activities across federal agencies and the private sector. Further, the Department of Homeland Security (DHS) lacks processes needed to address specific weaknesses in sharing information on control system vulnerabilities. Until public and private sector security efforts are coordinated by an overarching strategy, there is an increased risk that multiple organizations will conduct duplicative work. In addition, until information-sharing weaknesses are addressed, DHS risks not being able to effectively carry out its responsibility for sharing information on vulnerabilities with the private and public sectors.

GAO Recommendations to DHS

- Develop a strategy to guide efforts for securing control systems, including agencies' responsibilities, as well as overall goals, milestones, and performance measures.
- Establish a rapid and secure process for sharing sensitive control system vulnerability information with critical infrastructure control system stakeholders, including vendors, owners, and operators.

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to join today's hearing on the cyber threat to control systems. Control systems perform vital functions in many of our nation's critical infrastructures, including electric power generation, transmission, and distribution; oil and gas refining and pipelines; water treatment and distribution; chemical production and processing; railroads and mass transit; and manufacturing.

In 2003, the *National Strategy to Secure Cyberspace*[1] reported that the disruption of control systems could have significant consequences for public health and safety and made securing these systems a national priority. This strategy further states that both the private and public sectors have a role in securing control systems and directs the Department of Homeland Security (DHS), in coordination with the Department of Energy (DOE) and other agencies, to work in partnership with private industry in increasing awareness of the importance of efforts to secure control systems, developing standards, and improving policies with respect to control systems security.

As requested, our testimony summarizes portions of a report being released today that discusses (1) the cyber threats, vulnerabilities, and the potential impact of attacks on critical infrastructure control systems; (2) private sector initiatives to strengthen the cyber security of control systems; and (3) the adequacy of public sector initiatives to strengthen the cyber security of control systems.[2] All the work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

[1] The White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).

[2] GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain,* GAO-07-1036, (Washington, D.C.: Oct. 17, 2007).

Results in Brief

Critical infrastructure control systems face increasing risks due to cyber threats, system vulnerabilities, and the serious potential impact of attacks as demonstrated by reported incidents. Threats can be intentional or unintentional, targeted or nontargeted, and can come from a variety of sources. Control systems are more vulnerable to cyber attacks than they were in the past for several reasons, including their increased connectivity to other systems and the Internet. Further, as demonstrated by past attacks and incidents involving control systems, the impact on a critical infrastructure could be substantial. For example, in 2006, a foreign hacker was reported to have planted malicious software[3] capable of affecting a water filtering plant's water treatment operations; and, also in 2006, excessive traffic on a nuclear power plant's control system network—possibly caused by the failure of another control system device—caused two circulation pumps to fail, forcing the unit to be shut down manually.

Multiple private sector entities such as trade associations and standards setting organizations specific to the electric, chemical, oil and gas, and water sectors are working to help secure control systems. These entities are developing standards, providing guidance to members, and hosting workshops on control systems security.

Over the past few years, federal agencies—including DHS, DOE, the National Institute of Standards and Technology (NIST), and others—have initiated efforts to improve the security of critical infrastructure control systems. However, there is as yet no overall strategy to coordinate the various control systems activities across federal agencies and the private sector. Further, DHS lacks processes needed to address specific weaknesses in sharing information on control system vulnerabilities. Until public and private sector security efforts are coordinated by an overarching

[3] "Malware" (malicious software) is defined as programs that are designed to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded into useful programs so that users are induced into activating them.

strategy, there is an increased risk that multiple organizations will conduct duplicative work and miss opportunities to learn from other organizations' activities. In addition, until information-sharing weaknesses are addressed, DHS risks not being able to effectively carry out its responsibility for sharing information on vulnerabilities with the private and public sectors.

Given the importance of these issues, in our report being released today, we are making recommendations to the Secretary of the Department of Homeland Security to (1) develop a strategy for coordinating control systems security efforts and (2) enhance information sharing with control systems stakeholders. In its comments on our report, DHS neither agreed nor disagreed with these recommendations, but stated that it would take them under advisement. The agency also discussed new initiatives to develop plans and processes that are consistent with our recommendations.

Background

Critical infrastructures are physical or virtual systems and assets so vital to the nation that their incapacitation or destruction would have a debilitating impact on national and economic security and on public health and safety. These systems and assets—such as the electric power grid, chemical plants, and water treatment facilities—are essential to the operations of the economy and the government. Recent terrorist attacks and threats have underscored the need to protect our nation's critical infrastructures. If vulnerabilities in these infrastructures are exploited, our nation's critical infrastructures could be disrupted or disabled, possibly causing loss of life, physical damage, and economic losses.

Although the vast majority of our nation's critical infrastructures are owned by the private sector, the federal government owns and operates key facilities that use control systems, including oil, gas, water, energy, and nuclear facilities.

Control Systems Are Used in Many Critical Infrastructures

Control systems are computer-based systems that are used within many infrastructures and industries to monitor and control sensitive processes and physical functions. Typically, control systems collect sensor measurements and operational data from the field, process and display this information, and relay control commands to local or remote equipment. Control systems perform functions that range from simple to complex. They can be used to simply monitor processes—for example, the environmental conditions in a small office building—or to manage the complex activities of a municipal water system or a nuclear power plant.

In the electric power industry, control systems can be used to manage and control the generation, transmission, and distribution of electric power. For example, control systems can open and close circuit breakers and set thresholds for preventive shutdowns. The oil and gas industry uses integrated control systems to manage refining operations at plant sites, remotely monitor the pressure and flow of gas pipelines, and control the flow and pathways of gas transmission. Water utilities can remotely monitor well levels and control the wells' pumps; monitor flows, tank levels, or pressure in storage tanks; monitor water quality characteristics such as pH, turbidity, and chlorine residual; and control the addition of chemicals to the water.

Installing and maintaining control systems requires a substantial financial investment. DOE cites research estimating the value of the control systems used to monitor and control the electric grid and the oil and natural gas infrastructure at $3 billion to $4 billion.[4] The thousands of remote field devices represent an additional investment of $1.5 billion to $2.5 billion. Each year, the energy sector alone spends over $200 million for control systems, networks, equipment, and related components and at least that amount in personnel costs.

[4] Newton-Evans Research Company, Inc., *World Market Study of SCADA, Energy Management Systems and Distribution Management Systems in Electrical Utilities: 2005-2007*, (Ellicott City, Maryland: June 2005) as cited in U.S. Department of Energy, *Roadmap to Secure Control Systems in the Energy Sector* (Washington, D.C.: January 2006).

Control Systems: Types and Components

There are two primary types of control systems: distributed control systems and supervisory control and data acquisition (SCADA) systems. Distributed control systems typically are used within a single processing or generating plant or over a small geographic area, while SCADA systems typically are used for large, geographically dispersed operations. For example, a utility company may use a distributed control system to manage power generation and a SCADA system to manage its distribution.

A SCADA system is generally composed of six components: (1) instruments, which sense conditions such as pH, temperature, pressure, power level, and flow rate; (2) operating equipment, which includes pumps, valves, conveyors, and substation breakers; (3) local processors, which communicate with the site's instruments and operating equipment, collect instrument data, and identify alarm conditions; (4) short-range communication, which carry analog and discrete signals between the local processors and the instruments and operating equipment; (5) host computers, where a human operator can supervise the process, receive alarms, review data, and exercise control; and (6) long-range communications, which connect local processors and host computers using, for example, leased phone lines, satellite, and cellular packet data.

The Federal Government Plays a Critical Role in Helping Secure Critical Infrastructures and Their Control Systems

Several key federal plans focus on securing critical infrastructure control systems. *The National Strategy to Secure Cyberspace*[5] calls for DHS and DOE to work in partnership with industry to develop best practices and new technology to increase the security of critical infrastructure control systems, to determine the most critical control systems-related sites, and to develop a prioritized plan for short-term cyber security improvements for those sites. In addition, DHS's *National Infrastructure Protection Plan*[6] specifically identifies

[5] The White House*, The National Strategy to Secure Cyberspace*.

[6] Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, D.C.: June 2006).

control systems as part of the cyber infrastructure, establishes an objective of reducing vulnerabilities and minimizing the severity of attacks on these systems, and identifies programs directed at protecting control systems. Further, in May 2007, the critical infrastructure sectors issued sector-specific plans to supplement the *National Infrastructure Protection Plan*. Twelve sectors, including the chemical, energy, water, information technology, postal, emergency services, and telecommunications sectors, identified control systems within their respective sectors. Of these, most identified control systems as critical to their sector and listed efforts under way to help secure them.

Critical Infrastructure Control Systems Face Increasing Risks Due to Cyber Threats, Vulnerabilities, and the Potentially Serious Impact of an Attack

Cyber threats can be intentional and unintentional, targeted or nontargeted, and can come from a variety of sources. Intentional threats include both targeted and nontargeted attacks, while unintentional threats can be caused by software upgrades or maintenance procedures that inadvertently disrupt systems. A targeted attack is when a group or individual specifically attacks a critical infrastructure system and a nontargeted attack occurs when the intended target of the attack is uncertain, such as when a virus, worm, or malware is released on the Internet with no specific target.

There is increasing concern among both government officials and industry experts regarding the potential for a cyber attack on a national critical infrastructure, including the infrastructure's control systems. The Federal Bureau of Investigation has identified multiple sources of threats to our nation's critical infrastructures, including foreign nation states engaged in information warfare, domestic criminals, hackers, and virus writers, and disgruntled employees working within an organization.

Control Systems Are Vulnerable to Cyber Attacks

Control systems are vulnerable to flaws or weaknesses in system security procedures, design, implementation, and internal controls. When these weaknesses are accidentally triggered or intentionally exploited, they could result in a security breach. Vulnerabilities could occur in control systems' policies, platform (including hardware, operating systems, and control system applications), or networks.

Federal and industry experts believe that critical infrastructure control systems are more vulnerable today than in the past due to the increased standardization of technologies, the increased connectivity of control systems to other computer networks and the Internet, insecure connections, and the widespread availability of technical information about control systems. Further, it is not uncommon for control systems to be configured with remote access through either a dial-up modem or over the Internet to allow remote maintenance or around-the-clock monitoring. If control systems are not properly secured, individuals and organizations may eavesdrop on or interfere with these operations from remote locations.

Reported Control Systems Incidents Reveal the Potential for Substantial Impact

Reported attacks and unintentional incidents involving critical infrastructure control systems demonstrate that a serious attack could be devastating. Although there is not a comprehensive source for incident reporting, the following examples, reported in government and media sources,[7] demonstrate the potential impact of an attack.

[7] See National Institute of Standards and Technology, *Special Publication 800-82 Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security: Recommendations of the National Institute of Standards and Technology,* (Gaithersburg, Maryland: September 2006); Los Angeles County District Attorneys Office (da.co.la.ca.us/mr/010507a.htm), *Two City Engineers Charged with Allegedly Hacking Into City's Traffic Computer* (Los Angeles, California: Jan. 5, 2007); and ISA (www.isa.org/content/contentgroups/news/2006/november29/hackers_hit_pennsylvania_water_system.htm), *Hackers Hit Pennsylvania Water System,* (Research Triangle Park, North Carolina: Nov. 2, 2006).

- **Bellingham, Washington, gasoline pipeline failure**. In June 1999, 237,000 gallons of gasoline leaked from a 16-inch pipeline and ignited an hour and a half later, causing three deaths, eight injuries, and extensive property damage. The pipeline failure was exacerbated by poorly performing control systems that limited the ability of the pipeline controllers to see and react to the situation.

- **Maroochy Shire sewage spill**. In the spring of 2000, a former employee of an Australian software manufacturing organization applied for a job with the local government, but was rejected. Over a 2-month period, this individual reportedly used a radio transmitter on as many as 46 occasions to remotely break into the controls of a sewage treatment system. He altered electronic data for particular sewerage pumping stations and caused malfunctions in their operations, ultimately releasing about 264,000 gallons of raw sewage into nearby rivers and parks.

- **CSX train signaling system.** In August 2003, the Sobig computer virus shut down train signaling systems throughout the East Coast of the United States. The virus infected the computer system at CSX Corporation's Jacksonville, Florida, headquarters, shutting down signaling, dispatching, and other systems. According to an Amtrak spokesman, 10 Amtrak trains were affected. Train service was either shut down or delayed up to 6 hours.

- **Los Angeles traffic lights.** According to several published reports, in August 2006, two Los Angeles city employees hacked into computers controlling the city's traffic lights and disrupted signal lights at four intersections, causing substantial backups and delays. The attacks were launched prior to an anticipated labor protest by the employees.

- **Harrisburg, Pennsylvania, water system.** In October 2006, a foreign hacker penetrated security at a water filtering plant. The intruder planted malicious software that was capable of affecting the plant's water treatment operations. The infection occurred through the Internet and did not seem to be a direct attack on the control system.

- **Browns Ferry power plant.** In August 2006, two circulation pumps at Unit 3 of the Browns Ferry, Alabama, nuclear power plant failed, forcing the unit to be shut down manually. The failure of the pumps was traced to excessive traffic on the control system network, possibly caused by the failure of another control system device.

As control systems become increasingly interconnected with other networks and the Internet, and as the system capabilities continue to increase, so do the threats, potential vulnerabilities, types of attacks, and consequences of compromising these critical systems.

The Private Sector Has Multiple Initiatives Under Way to Help Secure Control Systems

Industry-specific organizations in various sectors, including the electricity, oil and gas, and water sectors, have initiatives under way to help improve control system security, including developing standards and publishing guidance. Our report being released today provides a detailed list of industry initiatives; several of these initiatives are described below.

- **Electricity.** In 2007, the North American Electric Reliability Corporation began implementing cyber security reliability standards that apply to control systems and the Institute of Electrical and Electronics Engineers has several standards working groups addressing issues related to control systems security in the industry.

- **Oil and gas.** The American Gas Association supported development of a report that would recommend how to apply encryption to protect gas utility control systems; and, over the past three years, the American Petroleum Institute has published two standards related to pipeline control systems integrity and security and the design and implementation of control systems displays.

- **Water.** The water sector includes about 150,000 water, wastewater, and storm water organizations at all levels of government and has worked with the Environmental Protection Agency on development of the Water Sector-Specific Plan, which includes some efforts on control systems security. In addition, the Awwa Research Foundation is currently working on two research projects related to the cyber security of water utility SCADA systems.

Federal Agencies Have Multiple Initiatives to Help Secure Critical Infrastructure Control Systems, but More Remains to Be Done

Over the past few years, federal agencies— including DHS, DOE, and others—have initiated efforts to improve the security of critical infrastructure control systems. For example, DHS is sponsoring multiple control systems security initiatives, including the Control System Cyber Security Self Assessment Tool, an effort to improve control systems' cyber security using vulnerability evaluation and response tools, and the Process Control System Forum, to build relationships with control systems' vendors and infrastructure asset owners. Additionally, DOE sponsors control systems security efforts within the electric, oil, and natural gas industries. These efforts include the National SCADA Test Bed Program, which funds testing, assessments, and training in control systems security, and the development of a road map for securing control systems in the energy sector. Our report being released today provides a more detailed list of initiatives being led by federal agencies.

DHS, however, has not yet established a strategy to coordinate the various control systems activities across federal agencies and the private sector. In 2004, we recommended that DHS develop and implement a strategy for coordinating control systems security efforts among government agencies and the private sector.[8] DHS agreed and issued a strategy that focused primarily on DHS's initiatives. The strategy does not include ongoing work by DOE, the Federal Energy Regulatory Commission, NIST, and others. Further, it does not include the various agencies' responsibilities, goals, milestones, or performance measures. Until DHS develops an overarching strategy that delineates various public and private entities' roles and responsibilities and uses it to guide and

[8] GAO, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems,* GAO-04-354, (Washington, D.C.: Mar. 15, 2004).

coordinate control systems security activities, the federal government and private sector risk investing in duplicative activities and missing opportunities to learn from other organizations' activities.

Further, DHS is responsible for sharing information with critical infrastructure owners on control systems vulnerabilities, but lacks a rapid, efficient process for disseminating sensitive information to private industry owners and operators of critical infrastructures. An agency official noted that sharing information with the private sector can be slowed by staff turnover and vacancies at DHS, the need to brief agency and executive branch officials and congressional staff before briefing the private sector, and difficulties in determining the appropriate classification level for the information. Until the agency establishes an approach for rapidly assessing the sensitivity of vulnerability information and disseminating it—and thereby demonstrates the value it can provide to critical infrastructure owners—DHS's ability to effectively serve as a focal point in the collection and dissemination of sensitive vulnerability information will continue to be limited. Without a trusted focal point for sharing sensitive information on vulnerabilities, there is an increased risk that attacks on control systems could cause a significant disruption to our nation's critical infrastructures.

Implementation of GAO Recommendations Would Help Improve Federal Control Systems Security Efforts

Control systems are an essential component of our nation's critical infrastructure and their disruption could have a significant impact on public health and safety. Given the importance of control systems, in our report being released today, we are recommending that the Secretary of the Department of Homeland Security implement the following two actions:[9]

[9] GAO-07-1036.

- develop a strategy to guide efforts for securing control systems, including agencies' responsibilities, as well as overall goals, milestones, and performance measures and

- establish a rapid and secure process for sharing sensitive control system vulnerability information with critical infrastructure control system stakeholders, including vendors, owners, and operators.

In its comments on our report, DHS neither agreed nor disagreed with these recommendations, but stated that it would take them under advisement. The agency also discussed new initiatives to develop plans and processes that are consistent with our recommendations.

In summary, past incidents involving control systems, system vulnerabilities, and growing threats from a wide variety of sources highlight the risks facing control systems. The public and private sectors have begun numerous activities to improve the cyber security of control systems. However, the federal government lacks an overall strategy for coordinating public and private sector efforts. DHS also lacks an efficient process for sharing sensitive information on vulnerabilities with private sector critical infrastructure owners.

Until DHS completes the comprehensive strategy, the public and private sectors risk undertaking duplicative efforts. Further, without a streamlined process for advising private sector infrastructure owners of vulnerabilities, DHS is unable to fulfill its responsibility as a focal point for disseminating this information. If key vulnerability information is not in the hands of those who can mitigate its potentially severe consequences, there is an increased risk that attacks on control systems could cause a significant disruption to our nation's critical infrastructures.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you or members of the subcommittee may have at this time.

If you have any questions on matters discussed in this testimony, please contact me at (202) 512-6244, or by e-mail at wilshuseng@gao.gov. Other key contributors to this testimony include Scott Borre, Heather A. Collins, Neil J. Doherty, Vijay D'Souza, Nancy Glover, Sairah Ijaz, Patrick Morton, and Colleen M. Phillips (Assistant Director).